Presentation to the State Information Technology Advisory Committee (SITAC)

Presented by: Lisa Feldner, CIO
Information Technology Department

November 15, 2007
Dakota Carrier Network Building ~ Board Room

Welcome

- Annual Report
- Project Management Award
- IT Planning / Collaboration Meetings

STANDARDS / WAIVERS

Cathie Forsch
Director of Operations
ND Tax Department

CONNECTND UPDATE

Pam Sharp, Director
Office of Management & Budget

Large Project Reports

- Secretary of State ~ Al Jaeger
- Workforce Safety & Insurance ~ Jim Long

Large Project Report

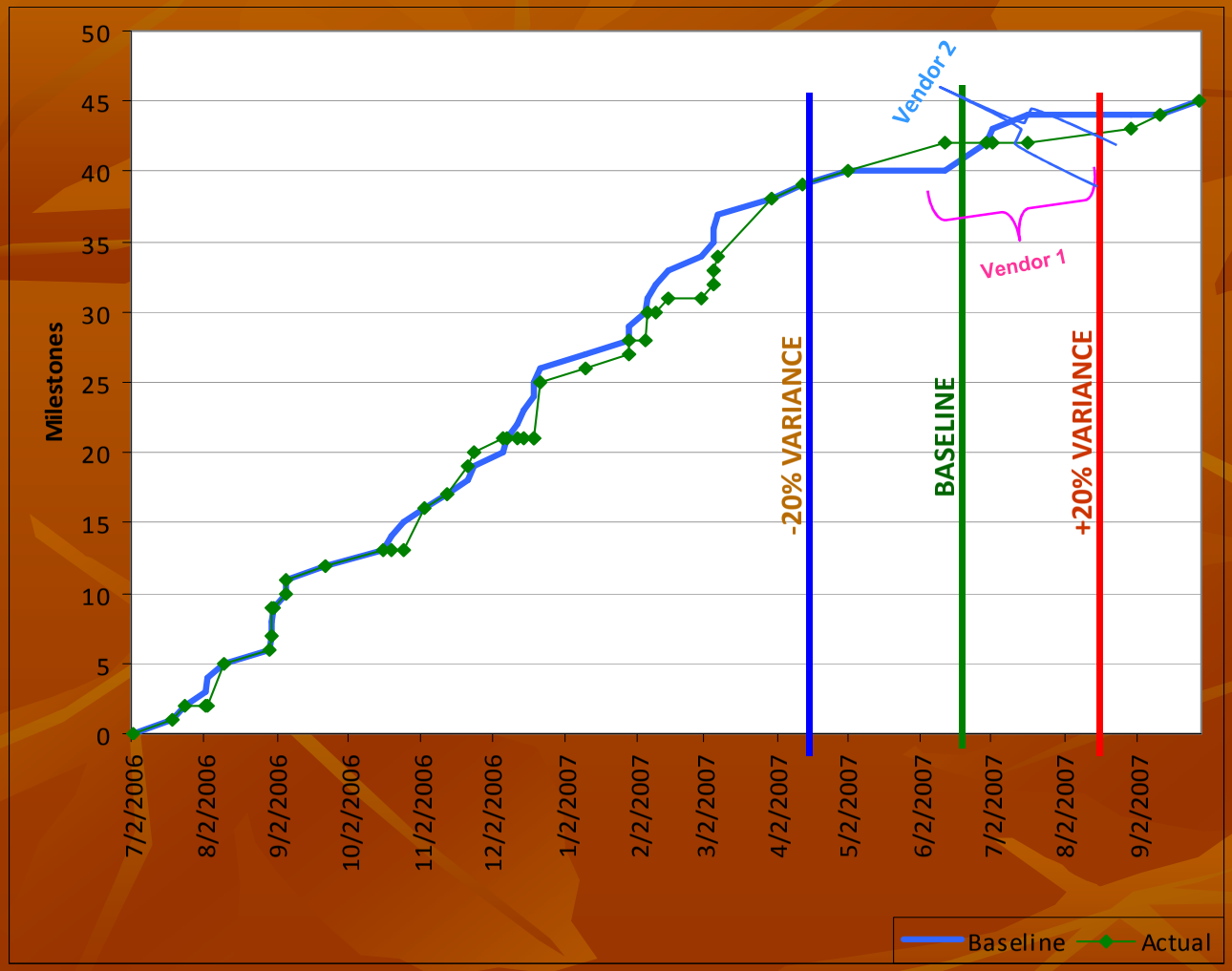
Secretary of State ~ Al Jaeger

Large Project Report

ITTP System Replacement Project

Workforce Safety & Insurance ~ Jim Long

Milestones and Timeline



- Baseline completion
- Time spent negotiating unsuccessfully with Deloitte Vendor 1
- Time spent successfully negotiating with Vendor 2

Vendor 1 Negotiation Problems

- "*32-12.2-15. Contracts limiting liability to the state - Assumption of certain excess liability by the risk management fund.* Notwithstanding any provision in this chapter to the contrary, if the attorney general and the director of the office of management and budget determine it is in the best interest of the state, an agency may agree to limit the liability of a contractor to the state. **The liability limitation must be approved by the attorney general and director of the office of management and budget in writing and may only be approved for contracts for the purchase or lease of software, communication, or electronic equipment.** For any uninsured losses, the director of the office of management and budget may approve the risk management fund to assume all or part of the contractor's liability to the state in excess of the limitation." (emphasis added)
- WSI applied to the Attorney General's office to limit the liability of Vendor 1. This request was denied because the purpose of the integration contract was to provide "services" and not "software."

Thank You

- Questions, comments

Break Time

INFORMATION TECHNOLOGY AUDIT REPORT

Don LaFleur/Mark Shaw
State Auditor's Office

Introduction

- **ManTech SMA Project Manager**

Mark Shaw
Principal Forensics and Intrusion Engineer
CFIA Cyber Defense Division
mark.shaw@mantech.com
(703)610-9326

Project Overview

- Security Assessment conducted August-September 2007
- 4 Project Tasks
  - External Vulnerability Assessment
  - Internal Vulnerability Assessment
  - Penetration Test
  - Application Security Assessment

External Vulnerability Assessment-Overview

- **Conducted August 13-22 2007**
- **Passive Mapping**
  - **Internet searches**
    - **Personnel (emails, phone numbers, key personnel)**
    - **Documents**
    - **Network Assets**
    - **WHOIS & DNS queries**
  - **Open source research is virtually undetectable by target**
  - **Information gathered is available to anyone**

External Vulnerability Assessment-Overview

- **Active Mapping**
  - **Port scanning**
    - **Identify available systems and services**
  - **Automated scanners and manual checks**
    - **Identify vulnerabilities**

External Vulnerability Assessment-Results

- **Vulnerability Findings**
  - **Great improvement over 2005 results**
  - **K12/EDU scanned but results not fully analyzed**
  - **313 systems State Agencies or organizations found to have at least one vulnerability**
  - **10 high risk/2 medium risk/4 low risk**
  - **Vulnerabilities could be classified as:**
    - **Missing OS or Application Patches**
    - **Architectural Design**
    - **Misconfigured Systems or Applications**

External Vulnerability Assessment-Results

- **General Recommendations**
  - **Review Content Available on Publicly Accessible Servers**
  - **Filter Inbound Access to All State Systems**
  - **Ensure Segregation Between K12/EDU and State Networks**

Internal Vulnerability Assessment-Overview

- **Conducted August 27-September 5 2007**
- **Similar Methodology to External Assessment**
- **Identify vulnerabilities and security misconfigurations**
- **Automated scanners and manual checks**
  - **Identify risks to systems and data**

Internal Vulnerability Assessment-Results

- **Vulnerability Findings**
  - **Great improvement over 2005 results**
  - **427 systems at State Agencies or organizations found to have at least one vulnerability**
  - **29 high risk/8 medium risk/4 low risk**
  - **Vulnerabilities could be classified as:**
    - **Missing OS or Application Patches**
    - **Architectural Design**
    - **Misconfigured Systems or Applications**

Internal Vulnerability Assessment-Results

- **General Recommendations**
  - **Segment Public Facing Servers from Internal Network**
  - **Internal Segregation of Critical Servers and Development Systems**
  - **Include Applications in Formal Patch Management Program**
  - **Implement Outbound Access Control**
  - **Require use of Encrypted Protocols for Remote Management**

Penetration Test-Overview

- Conducted September 5-10 2007
- Emulate realistic & current threats
  - Gain access to systems
    - Technical means & social engineering
- Exploit discovered vulnerabilities
  - Find legitimate vulnerabilities not identified by conventional methods
  - Fully Validate findings
- Test Response Procedures

Penetration Test-Overview

- **Social Engineering**
  - **Gain access to systems and/or information**
  - **Sensitize user population and administrators to hacker techniques**
    - **Phishing**
    - **Client-side exploits**
    - **Pretexting**

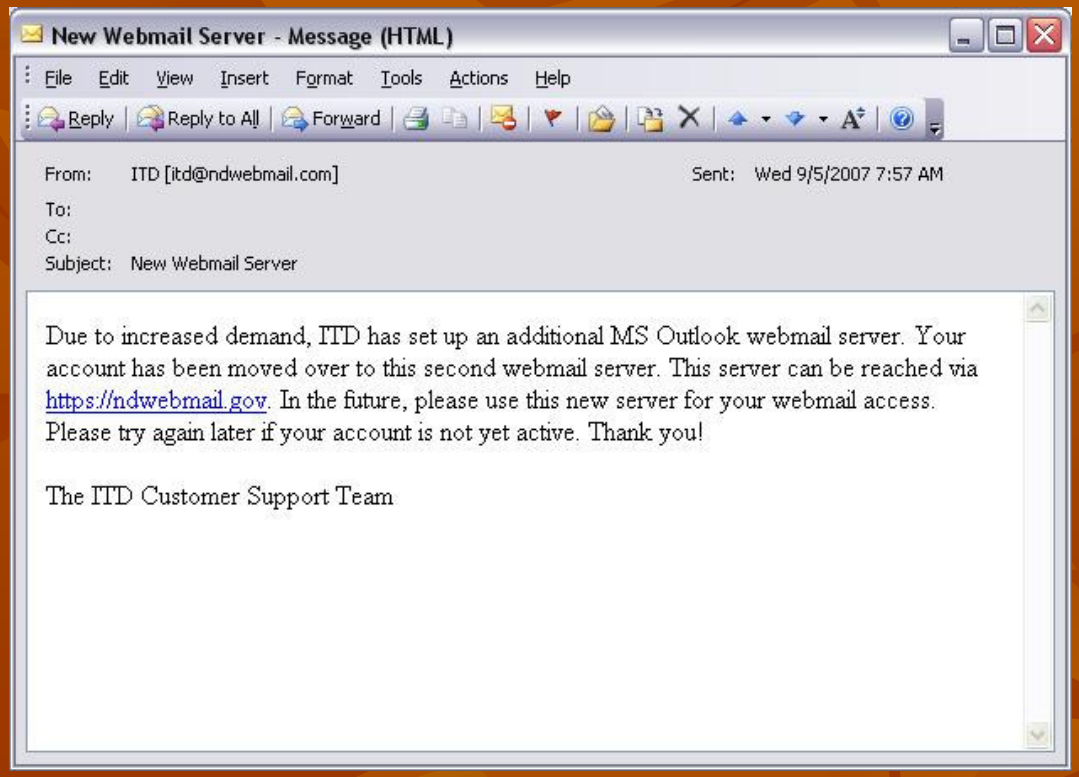
Penetration Test-Results

- **Direct Exploitation**
  - **Identified 9 systems to target based on vulnerability assessment results**
  - **Unsuccessful in exploiting 8 of the systems**
  - **Successfully exploited one system and created an account with administrator privileges**

Penetration Test-Results

Phishing email #1

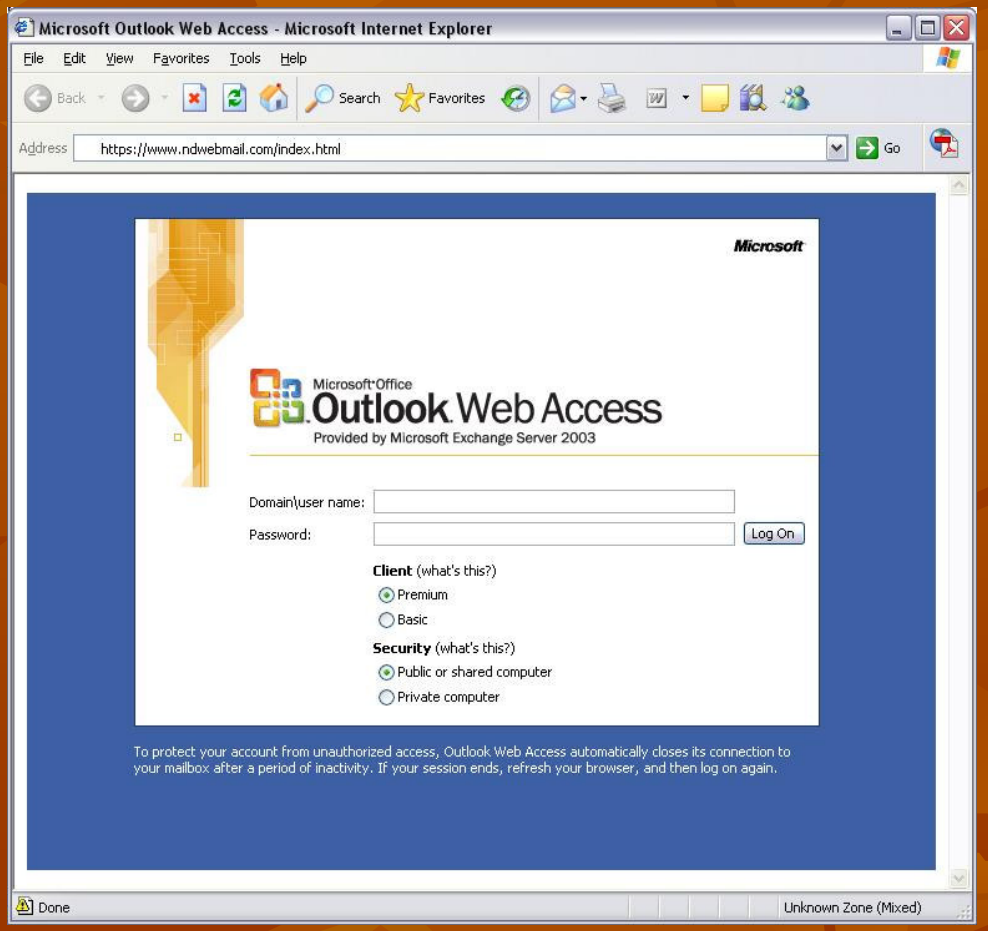
- ndwebmail.com domain
- Sent ~110 emails from "ITD"
- Directs users to "new" web mail site



Penetration Test-Results

Phishing email #1

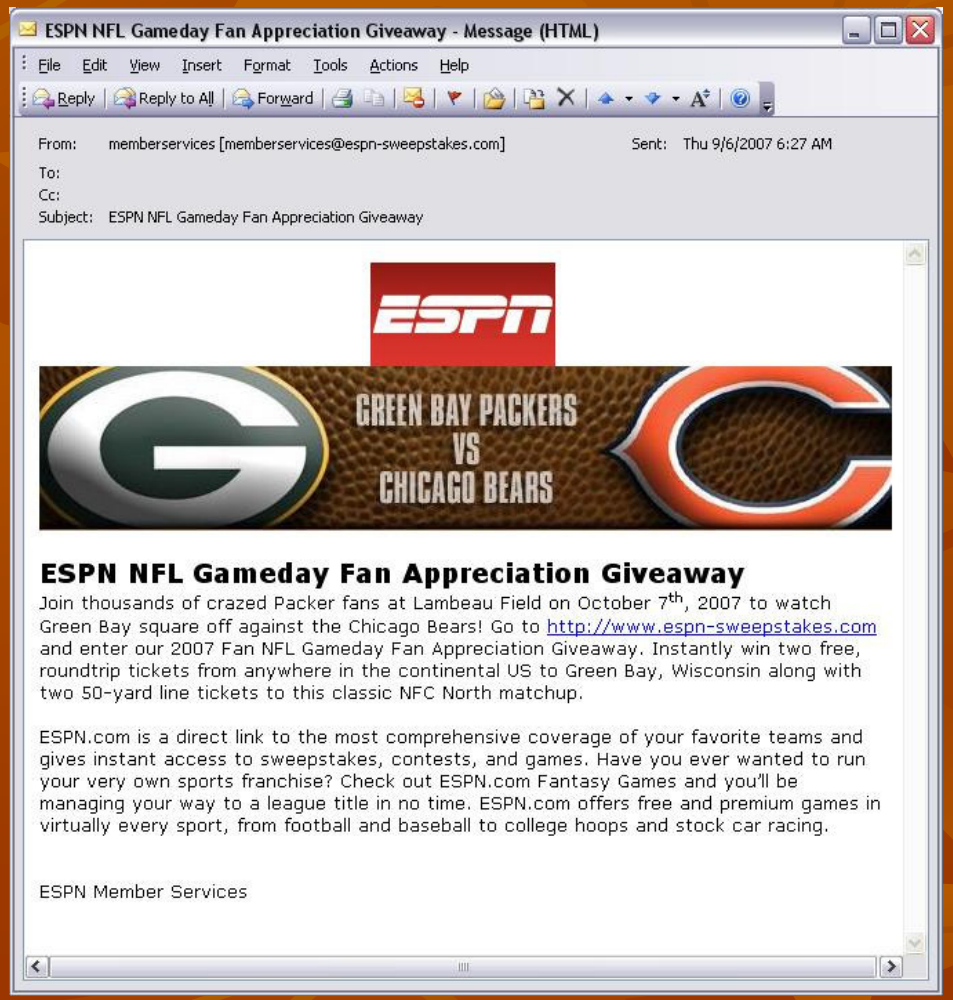
- Fake OWA site controlled by Test Team
- SSL encrypted
- 1 user entered credentials
- Reported to ITD within 3 hours of first email being sent
- ITD notified users of fraudulent email



Penetration Test- Results

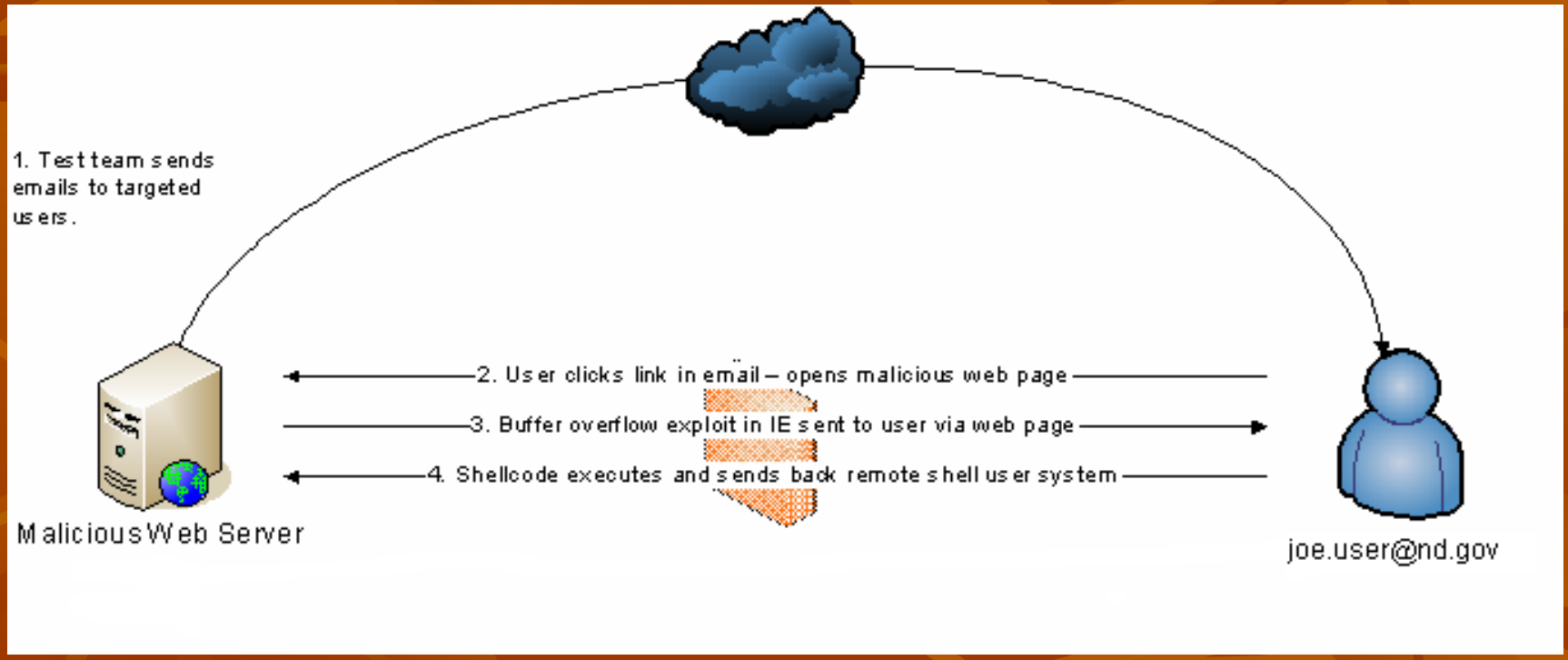
Phishing email #2

- Sweepstakes offer from "ESPN"
- Sent ~330 emails
- Directs users to malicious website
- 7 different attempts to access webpage
- No successful exploits
- Email not reported



Penetration Test- Results

Phishing email #2



Penetration Testing Results

- **General Recommendations**
  - **Education of users on social engineering techniques**
  - **Ensure servers and desktops kept current on all operating system and application patches**

Application Security Assessment-Overview

- **Conducted August 22-September 5 2007**
- **Targeted PeopleSoft Financials application**
- **End-to-End Assessment of all Application Components**
- **Automated scanners and manual checks**

Application Security Assessment-Results

- **Vulnerability Findings**
  - **Security of the application is very strong**
  - **1 high risk/1 low risk**
  - **Vulnerabilities could be classified as:**
    - **Missing OS or Application Patches**
    - **Architectural Design**

Application Security Assessment- Results

- **General Recommendations**
  - **Ensure systems hosting application are kept up to date**
  - **Prevent simultaneous logins**

QUESTIONS

Wrap Up

- SPAM filtering
- Other Updates
- Future meeting topics
  - State Portal

THANK YOU